Survivable Authentication for Health Information Systems

Kemal Bicakci, M.S. and Nazife Baykal, Ph.D.
Middle East Technical University, Informatics Institute, Ankara, TURKEY

ABSTRACT

Possible solutions to establish a survivable authentication framework in a health information system including the one based on one-time passwords (OTPs) are discussed. A new convenient method to generate OTPs is proposed.

INTRODUCTION

Since passwords by itself does not provide the security level most systems require, strong authentication is established by the use of at least two kinds of evidence at least one of which is resistant to replay. This motivates to use special hardware **(smartcards)** for the authentication framework for e-health systems since the only method not relying on special hardware, which is resistant to replay, is the inconvenient one-time passwords (OTPs). However, we claim there is a problem what we call **survivability** in using special hardware for the authentication in a health information system since there is a significant risk in locations where there is no smartcard reader available such as on an airplane or in a foreign country. For instance, suppose that a patient gets sick while he is in a visit to a foreign country, his doctor traveling with him needs to reach the patient's health record stored in a central database but there is not any smart card reader operational at that moment. What does he do now? This problem is precisely the topic of this poster.

SOLUTIONS FOR SURVIVABILITY

Solutions to overcome this limitation of smart-card based authentication are as follows:

Off-line override: The doctor calls the system admin of patient record database and asks him for help. The main limitation of this method is its susceptibility of attacks known as social engineering. This attack on medical record privacy usually comes from a private detective who phones with a plausible tale asking about a person's record claiming that there is an emergency situation. This kind of attack is usually so successful that in both United States and Britain there are people who earn their living doing it.

Password-only method: Using only password authentication when there is no smart card reader has serious drawbacks. The most serious one is the security concerns.

Cryptographic calculators: A cryptographic calculator is like a smartcard that it performs cryptographic calculations using a key that it will not disclose. It is unlike a smart card in that it requires no electrical connection to the terminal. It has a display and a keyboard, and all interaction is through the user. The disadvantages of having a cryptographic calculator supplement to the smart card for survivability reasons is two-folds. First, it is infeasible to spend money on two separate devices (smartcard and calculator). Second, carrying a second device and interact with it manually is not much more convenient than using one-time passwords.

THE PROPOSED SOLUTION: Our solution to have a survivable authentication system is based on OTPs. The system then would work as follows: OTPs are written down on a piece of paper or alternatively, mobile devices such as PDAs and cellular phones are used for storing the OTP list. In order to be authenticated using devices without a smartcard reader, users enter the correct OTP to the system manually. This is somehow an inconvenience for the user but that inconvenience is worth in order to be authenticated and reach critical information securely in most medical emergency scenarios. The inconvenience of OTPs in fact is useful to facilitate secure authentication using smart tokens in usual operation.

Several OTP schemes have been proposed in the past but all of them require a setup (initialization) phase between the server and user(s). This is inflexible and inconvenient for the user himself as well as a bottleneck for the server. We now introduce our method to generate infinite number of OTPs without requiring the user to interact with the server beforehand. Our method is based on the public-key cryptography which has already been in use for the smartcard based authentication therefore our method provides seamless integration of OTPs and smart cards.

Construction: Let algorithm S be a signing algorithm in a signature scheme (e.g. RSA) where d is the private key (the corresponding public key is known by the server). $S_d^N(x)$ denotes that we apply the signing algorithm S recursively N times to the initial input x (not a shared secret, can be generated from the public key by a public algorithm). As seen below, recursive applications results in an (infinite length) OTPs originate from the initial input x:

$$x, S_d(x), S_d^2(x), S_d^3(x), \Lambda\ , S_d^N(x), S_d^{N+1}(x), \Lambda$$